REMARKS/DISCUSSION OF ISSUES

Claims 2-4 and 6-14 are pending in the application.

Reexamination and reconsideration are respectfully requested in view of the following Remarks.

35 U.S.C. § 103

The Office Action rejects claims 2, 4, 7, and 9-13 under 35 U.S.C. § 103 over Patarin et al. U.S. Patent 6,658,569 ("Patarin") in view of Jahnich et al. U.S. Patent 6,725,374 ("Jahnich"), and claims 8 and 14 under 35 U.S.C. § 103 Patarin over in view of Jahnich and further in view of Tan U.S. Patent 6,490,353 ("Tan").

Applicants respectfully traverse these questions for at least the following reasons.

Claim 2

Among other things, in the method of claim 2, a first processor performs useful cryptographic operations while a second processor, simultaneously and in parallel, performs dummy cryptographic operations which are discarded, so that consumption characteristics of the data-processing device are a superimposition of consumption characteristics associated with performing both the useful and the dummy cryptographic operations.

Applicants respectfully submit that no combination of the teachings of Patarin and Jahnich would produce such a method.

The Office Action states that Patarin discloses using two or more processors for performing cryptographic operations in parallel, and that Jahnich discloses using dummy operations.

However, even if one combined Patarin and Jahnich, one would not produce a method where a first processor performs useful cryptographic operations while a second processor, simultaneously and in parallel, performs dummy cryptographic operations which are discarded, so that consumption characteristics of the data-processing device are a superimposition of consumption characteristics associated with performing both the useful and the dummy cryptographic operations. That is

because neither Patarin nor Jahnich teaches or suggests the division or segregation of useful operations from dummy operations, so that the useful operations are performed with a first processor and the dummy operations are performed separately and independently (in parallel and simultaneously) with a separate second processor.

At best, a combination of Patarin and Jahnich would produce a method where useful and dummy operations are performed using the two or more processors of Patarin but are ***interspersed with each other in time***. This is evident from Jahnich's specific teaching that useful and dummy operations should be "*randomly distributed over time*" to impede a DPA attack (see, e.g., col. 6, lines 43-48; col. 4, lines 8-13; col. 6, lines; col. 5, lines 19-25). Anything else would be directly contrary to the teachings of Jahnich which explicitly advocates interspersing useful and dummy operation sin time, not executing them simultaneously!

So, a combination of Patarin and Jahnich would not produce a method where a first processor performs useful cryptographic operations while a second processor, simultaneously and in parallel, performs dummy cryptographic operations which are discarded. Also, because useful and dummy operations are interspersed with each other in time, a combination of Patarin and Jahnich would not produce a method where consumption characteristics of the data-processing device are a superimposition of consumption characteristics associated with performing both useful and rejected cryptographic operations.

Therefore, no combination of Patarin and Jahnich would ever produce the method of claim 2.

Furthermore, Applicants respectfully traverse the proposed combination of Patarin and Jahnich as lacking proper motivation and being contrary to M.P.E.P. § 2143.01.

M.P.E.P. § 2143.01 provides that "*there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings.*"

Here, the Office Action states that the proposed motivation for modifying

Patarin's method to (supposedly) produce a method wherein a first processor performs useful cryptographic operations while a second processor, simultaneously and in parallel, performs dummy cryptographic operations which are discarded, is Jahnich's teaching to impede reconstruction of consumption characteristics associated with performing the cryptographic operation. However, this could not possibly provide any motivation for modifying Patarin's method to produce a method wherein a first processor performs useful cryptographic operations while a second processor, simultaneously and in parallel, performs dummy cryptographic operations which are discarded would be impeded, because Jahnich clearly and specifically teaches that in order to impede reconstruction of consumption characteristics associated with performing the cryptographic operation, useful and dummy operations should be ***interspersed with each other in time***. There is nothing at all in Jahnich suggesting that useful and dummy cryptographic operations should be performed simultaneously and in parallel – indeed, such a teaching would be directly contrary to Jahnich's teachings.

Therefore, the "motivation" offered in the Office Action would never lead one to make the proposed combination, and is therefore no motivation at all for the proposed combination.

Furthermore, M.P.E.P. § 2143.01(VI) provides that "*if the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious*." Here, the proposed modification would completely destroy the principle of operation of Jahnich. In particular, Jahnich's fundamental principle of interspersing useful and dummy operations with each other in time would be fundamentally destroyed by performing the operations simultaneously and in parallel, as recited in claim 2.

RESPONSE TO RESPONSE TO ARGUMENTS

The "Response to Arguments" Section of the Office Action dated 27 February 2008 states that in Jahnich: "*Because the dummy operations are not executed in a fix*

(sic) order, it does not mean that they cannot be executed simultaneously with useful operations.""

At the outset, even assuming *arguendo* that everything said here was true, the fact that a reference does not teach that it cannot possibly be modified to operate in the manner of a claimed invention does not mean that it would have been obvious to have made such a modification. The test is whether there is an objective reason for the modification that can be supported by evidence in the record. Here, no such reason exists.

Jahnich very specifically, consistently, and repeatedly teaches that its useful crypto operations and its dummy operations should be randomly distributed in a **sequential** arrangement: "*parallelisationable subprograms which, however, **are executed sequentially in the portable data carrier**;*" (col. 2, lines 3-5); "*randomly permuting a **serial order** of execution of at least two of a plurality of parallelisationable subprograms*;" (col. 2, lines 65-67); "*randomly permuting a **serial** order of execution" (col. 3, lines 11-12; 17)*; "*wherein the dummy program is included in the **serial** order subjected to the step of randomly permuting*;" (col. 3, lines 39-41), etc., etc. etc. See also claims 1, 9, 18 and 21 (serial operation is specifically recited in each and every claim of Jahnich!). Jahnich specifically teaches that:

> "The implementation of dummy subprograms and their random permutation does not only generate additional current fluctuations which have nothing to do with the actual encryption program, but, in addition, **appear randomly distributed over time, which further impedes a DPA attack**."

Jahnich at col. 6, lines 43-48.

The serial interspersal of useful operations and dummy operations is a key feature of Jahnich's teachings. As noted above, any proposed modification of Jahnich to perform the operations simultaneously and in parallel, as recited in claim

2, would clearly destroy Jahnich's fundamental principle of interspersing useful and dummy operations with each other in time, and is therefore directly contrary to the express provisions of M.P.E.P. § 2143.01(VI).

Furthermore, Jahnich teaches against any such modification. Simultaneous operations as recited in claim 2 require at least two processors, CPUs, coprocessors, etc. Meanwhile, Jahnich specifically teaches away from any solution that "*requires implementation of an additional electronic component*" as "***unacceptable***" (col. 2, lines 51-56).

The "Response to Arguments Section" of the Office Action also states that "*the combination of Patarin and Jahnich would have yielded predictable results to one of ordinary skill in the art at the time of the invention.*"

Applicants respectfully submit that the only thing that the combination of Patarin and Jahnich could have yielded would have been an arrangement wherein useful operations and dummy operations are interspersed with other in time - not an arrangement where useful operations and dummy operations are performed simultaneously and in parallel.

The plain fact is that the Office Action fails to cite any teaching anywhere in the prior art that remotely suggests that useful operations and dummy operations should be performed simultaneously and in parallel by different processors, CPUs and/or coprocessors . . .and the only reference cited for dummy operations, teaches the exact opposite.

Accordingly, for at least these reasons, Applicants respectfully submit that claim 2 is patentable over the cited prior art.

Claims 4, 7 and 9

Claims 4, 7 and 9 depend from claim 2 and are deemed patentable for at least the reasons set forth above with respect to claim 2.

Claim 10

Among other things, in the device of claim 10 at least two of the CPU and co-processors perform a cryptographic operation simultaneously and in parallel with at least one dummy operation, whereby consumption characteristics associated with

performing the respective cryptographic and dummy operations are superimposed so that reconstruction of the consumption characteristics associated with performing the cryptographic operation is impeded.

As explained above with respect to claim 2, Applicants respectfully submit that no combination of Patarin and Jahnich would produce a device where two processors perform a cryptographic operation simultaneously and in parallel with at least one dummy operation. Applicants also respectfully submit that there is no motivation for the specifically-proposed combination of Patarin and Jahnich which supposedly would produce the device of claim 10, and any such combination would not only change, but completely destroy Jahnich's fundamental principle of operation.

Accordingly, for at least these reasons, Applicants respectfully submit that claim 10 is patentable over the cited prior art.

Claims 11-13

Claims 11-13 depend from claim 10 and are deemed patentable for at least the reasons set forth above with respect to claim 10.

Claims 8 and 14

Claims 8 and 14 depend respectively from claims 2 and 10. Applicants respectfully submit that Tan does not remedy the shortcomings of Patarin and Jahnich as set forth above with respect to claims 2 and 10, and therefore claims 8 and 14 are deemed patentable for at least the reasons set forth above with respect to claims 2 and 10.

CONCLUSION

In view of the foregoing explanations, Applicants respectfully request that the Examiner reconsider and reexamine the present application, allow claims 2-4 and 6-14 and pass the application to issue. In the event that there are any outstanding matters remaining in the present application, the Examiner is invited to contact Kenneth D. Springer (Reg. No. 39,843) at (571) 283.0720 to discuss these matters.

If necessary, the Commissioner is hereby authorized in this reply to charge payment or credit any overpayment to Deposit Account No. 50-0238 for any

additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17, particularly extension of time fees.

Respectfully submitted,

VOLENTINE & WHITT

Date: 27 May 2008

By: _____
Kenneth D. Springer
Registration No. 39,843

VOLENTINE & WHITT
One Freedom Square
11951 Freedom Drive, Suite 1260
Reston, Virginia 20190
Telephone No.: (571) 283.0724
Facsimile No.: (571) 283.0740